This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - Adobe Acrobat / Adobe Reader Disclosure of Sensitive Information
  - Best Software SalesLogix Multiple Vulnerabilities
  - **Cisco Systems Secure Access Control Server Multiple Remote Vulnerabilities (Updated)**
  - CyberStrong eShop ASP Shopping Card Unspecified Cross-Site Scripting
  - Digicraft Yak! Directory Traversal
  - Dmxready Site Chassis Manager Cross-Site Scripting and SQL Injection Vulnerabilities
  - Ideal Science IdealBB Multiple Input Validation Errors
  - MailEnable Professional Denial of Service Vulnerabilities
  - Mavel ShixxNote 6.net Buffer Overflow in Font Field
  - Microsoft Cabarc Directory Traversal Flaw Allows Remote File Creation
  - Microsoft Internet Explorer Incorrect URL Display
  - Microsoft Operating System 'asycpict.dll' Denial of Service
  - Microsoft PowerPoint / Visio Viewer JPEG Processing Buffer Overflow
  - Microsoft Windows 2003 Default ACL Permissions Firewall Services
  - Microsoft Windows 2003 Services Default SACL Configuration
  - Microsoft Windows XP Weak Default Configuration
  - **Microsoft RPC Runtime Library Information Disclosure & Denial of Service (Updated)**
  - **Microsoft Windows Shell Remote Code Execution (Updated)**
  - **Microsoft SMTP Remote Code Execution (Updated)**
  - **Microsoft Internet Explorer Security Update (Updated)**
  - **Microsoft Excel Remote Code Execution (Updated)**
  - **Microsoft NetDDE Remote Code Execution (Updated)**
  - **Microsoft NNTP Remote Code Execution (Updated)**
  - **Microsoft Windows Security Update (Updated)**
  - **Microsoft Compressed (zipped) Folders Remote Code Execution (Updated)**
  - Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability
  - NatterChat Input Validation Hole Lets Remote Users Inject SQL Commands
  - Pinnacle ShowCenter Skin File Cross-Site Scripting Vulnerability
  - Sungard SCT Campus Pipeline Input Validation Error
  - Symantec Norton AntiVirus Unprivileged Auto-Protection Deactivation
  - viksoe.dk GMail Drive Discloses Information and Permits Unauthorized Access
- UNIX / Linux Operating Systems
  - Apache mod_ssl SSLCipherSuite Access Validation
  - **Apache Mod_Proxy Remote Buffer Overflow (Updated)**
  - **Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow (Updated)**
  - **Carnegie Mellon University Cyrus SASL Buffer Overflow & Input Validation (Updated)**
  - cPanel Backup & FrontPage Management Remote Arbitrary File Modifications
  - Federico David Sacerdoti Ansel Insecure Default Permissions
  - Gnofract 4 Remote Arbitrary Code Execution
  - LibTIFF Buffer Overflows
  - Martin Schoenert Unzoo Input Validation
  - **mpg123 'do_layer2() Function' Remote Buffer Overflow (Updated)**
  - **Mr. S.K. LHA Multiple Code Execution (Updated)**
  - Multiple Vendors MySQL Database Unauthorized GRANT Privilege
  - **Multiple LHA Buffer Overflow/ Directory Traversal Vulnerabilities (Updated)**
  - **Multiple Vendors CUPS Error_Log Password Disclosure (Updated)**
  - **Multiple Vendors CUPS Browsing Denial of Service (Updated)**
  - **Multiple Vendors LibXpm Image Decoding Multiple Remote Buffer Overflow (Updated)**
  - **MySQL Mysql_real_connect Function Remote Buffer Overflow (Updated)**
  - MySQL Remote Denial of Service
  - **MySQL Security Restriction Bypass & Remote Denial of Service (Updated)**
  - phpMyAdmin Remote Command Execution
  - **Multiple Vulnerabilities in libpng (Updated)**
  - ProFTPd Login Timing Account Disclosure
  - **Samba Remote Denials of Service (Updated)**
  - **SoX ".WAV" File Processing Buffer Overflow Vulnerabilities (Updated)**
  - **Squid Remote Denial of Service (Updated)**
  - **Sun Solaris Gzip File Access (Updated)**
  - **Sudo Information Disclosure (Updated)**
  - WeHelpBUS Input Validation
  - **Yukihiro Matsumoto Ruby CGI Session Management Unsafe Temporary File (Updated)**
- Multiple Operating Systems
  - 3Com OfficeConnect ADSL Wireless 11g Firewall Router Multiple Vulnerabilities
  - 3Com 3CRADSL72 ADSL Wireless Router Information Disclosure & Authentication Bypass
  - AliveSites Forum Multiple Unspecified Remote Input Validation
  - ASN1 Multiple Vulnerabilities
  - ClientExec Default Installation Information Disclosure
  - CoolPHP Multiple Remote Input Validation
  - DevoyBB Forum Multiple Unspecified Remote Input Validation
  - Express-Web Content Management System Cross-Site Scripting
  - FuseTalk Cross-Site Scripting
  - GoSmart Message Board Multiple Input Validation
  - **IBM DB2 Multiple Buffer Overflows (Updated)**
  - **Macromedia JRun Multiple Remote Vulnerabilities (Updated)**
  - **Motorola Wireless Router WR850G Authentication Circumvention (Updated)**
  - Multiple Networking Devices 'Secure' Cookie Attribute Failure

---

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Adobe Adobe Acrobat 6.01 and 6.02; Adobe Reader 6.01 and 6.02	A vulnerability exists which can be exploited by malicious people to disclose sensitive information. This is because embedded Macromedia flash files are executed in a local context. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Adobe Acrobat / Adobe Reader Disclosure of Sensitive Information	Medium	Secunia Advisory, SA12809, October 13, 2004
Best Software SalesLogix 6	Multiple vulnerabilities were reported in which a remote malicious user can gain administrative access on the application. A remote user can inject SQL commands, determine the installation path, determine passwords, and upload arbitrary files. The vendor has issued a fix, available at: http://support.saleslogix.com/ Proofs of Concept exploits have been published.	Best Software SalesLogix Multiple Vulnerabilities	High	SecurityTracker Alert ID: 1011769, October 18, 2004
Cisco Systems Access Control Server Solution Engine, Secure Access Control Server 3.2 (3), 3.2 (2), 3.2, Secure ACS for Windows Server 3.2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the web-based management interface (CSAdmin); a remote Denial of Service vulnerability exists when processing LEAP (Light Extensible Authentication Procotol) authentication requests when the device is configured as a LEAP RADIUS proxy; a vulnerability exists when handling NDS (Novell Directory Services) users, which could let a remote malicious user bypass authentication; and a vulnerability exists in the ACS administration web services, which could let a remote malicious user bypass authentication. Workaround and patches available at: http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml **Cisco has released an updated advisory that contains workaround details and updates to address these issues.** There is no exploit code required.	Secure Access Control Server Multiple Remote Vulnerabilities	Low/Medium (Medium if authentication can be bypassed)	Cisco Security Advisory, 61603, August 25, 2004 **Cisco Security Advisory, 61603, Revision 1.2, October 4, 2004**
CyberStrong eShop 4.6	An input verification vulnerability exists which can be exploited by malicious people to conduct Cross-Site Scripting attacks. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	CyberStrong eShop ASP Shopping Card Unspecified Cross-Site Scripting	High	Secunia Advisory ID, SA12842, October 15, 2004
Digicraft Software Yak! 2.1.2	An input verification vulnerability exists in the built-in FTP server, which may allow a remote malicious user to upload arbitrary code anywhere on the system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Digicraft Yak! Directory Traversal	Medium	SecuriTeam, October 18, 2004

DmxReady Dmxready Site Chassis Manager	Input verification vulnerabilities exist which can be exploited by malicious people to conduct Cross-Site Scripting and SQL injection attacks. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Dmxready Site Chassis Manager Cross-Site Scripting & SQL Injection Vulnerabilities	High	Secunia Advisory ID, SA12841, October 15, 2004
Ideal Science IdealBB Multiple 0.1.5.3	Several input validation vulnerabilities were reported that could allow a remote malicious user to can inject SQL commands, conduct Cross-Site Scripting attacks, and conduct HTTP response splitting attacks. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Ideal Science IdealBB Multiple Input Validation Errors	High	SecurityTracker Alert ID, 1011691, October 14, 2004
MailEnable MailEnable Professional 1.x	Two unspecified vulnerabilities have been reported which potentially can be exploited by malicious people to cause a Denial of Service. Update to version 1.5e available at: http://www.mailenable.com/download.html We are not aware of any exploits for this vulnerability.	MailEnable Professional Denial of Service Vulnerabilities	Low	Secunia Advisory ID, SA12815, October 14, 2004
Mavel d.o.o. Software Company ShixxNote 6.net	A buffer overflow vulnerability exists that could permit a remote malicious user to execute arbitrary code on the target system. It is reported that a remote user can supply a specially crafted value for the field that specifies the font. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mavel ShixxNote 6.net Buffer Overflow in Font Field	High	SecurityTracker Alert ID, 1011672, October 14, 2004
Microsoft Cabarc	An input validation vulnerability was reported in Microsoft Cabarc which could allow a remote malicious user to create or overwrite arbitrary files on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Cabarc Directory Traversal Flaw Allows Remote File Creation	Medium	SecurityFocus Bugtraq ID, 11376, October 12, 2004
Microsoft Internet Explorer	A security vulnerability was reported that may allow a malicious user to spoof a user's homepage website. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Incorrect URL Display	Medium	SecurityTracker Alert ID, 1011735, October 16, 2004
Microsoft asycpict.dll in Windows (Me), Windows (NT), Windows (95), Windows (98), Windows (2000), Windows (2003), Windows (XP)	A vulnerability was reported in 'asycpict.dll' in the processing of JPEG images in which a remote malicious user can cause a target user's system to crash. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Operating System 'asycpict.dll' Denial of Service	Low	SecurityTracker Alert ID, 1011706, October 15, 2004
Microsoft Microsoft Office Visio 2002 Viewer Microsoft Office PowerPoint 2003 Viewer Microsoft Office Visio 2003 Viewer	A vulnerability has been discovered in three Microsoft Office Viewers, which can be exploited by malicious people to compromise a user's system. Install the latest versions of the viewers available at: http://www.microsoft.com/downloads/ We are not aware of any exploits for this vulnerability.	Microsoft PowerPoint / Visio Viewer JPEG Processing Buffer Overflow	High	Secunia Advisory SA12671, October 12,2004
Microsoft Windows 2003	A potential vulnerably was reported in Windows 2003. The default access control lists for the Distributed Link Tracking and Internet Connection Firewall services allow authenticated malicious users to stop the services. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Microsoft Windows 2003 Default ACL Permissions Firewall Services	Low	SecurityTracker Alert ID, 1011627, October 12, 2004
Microsoft Windows 2003	It is reported that the default SACL access right settings for multiple Microsoft Windows 2003 services allow unprivileged local malicious users to start them. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Microsoft Windows 2003 Services Default SACL Configuration	Medium	SecurityFocus Bugtraq ID, 11387, October 15, 2004
Microsoft Windows XP Home SP2 Windows XP Media Center Edition SP2 Windows XP Professional SP2	A default configuration vulnerability exists that may allow malicious users to create a listening port to provide remote access to a vulnerable computer. This is due to a weakness in the Internet Connection Firewall (ICF). No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows XP Weak Default Configuration	Medium	SecurityFocus Bugtraq ID, 11410, October 13, 2004
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition; **Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0,**	An information disclosure and Denial of Service vulnerability exists when the RPC Runtime Library processes specially crafted messages. A malicious user who successfully exploited this vulnerability could potentially read portions of active memory or cause the affected system to stop responding. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-029.mspx **Avaya: Customers are advised to follow Microsoft's guidance for applying patches.**	Microsoft RPC Runtime Library Information Disclosure & Denial of Service CVE Name: CAN-2004-0569	Low	Microsoft Security Bulletin MS04-029, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **SecurityFocus,**

S3400 Message Application Server, S8100 Media Servers	**Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate()** We are not aware of any exploits for these vulnerabilities.			**October 18, 2004**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows Server 2003 Datacenter Edition, Windows 98, Windows 98 SE, Windows ME	A Shell vulnerability and Program Group vulnerability exists in Microsoft Windows. These vulnerabilities could allow remote code execution. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Shell Remote Code Execution CVE Names: CAN-2004-0214 CAN-2004-0572	High	Microsoft Security Bulletin MS04-037, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Note VU#543864, October 15, 2004**
Microsoft Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003	A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles Domain Name System (DNS) lookups. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx We are not aware of any exploits for this vulnerability.	Microsoft SMTP Remote Code Execution CVE Name: CAN-2004-0840	High	Microsoft Security Bulletin MS04-035, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Note VU#394792, October 15, 2004**
Microsoft Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6.0 for Windows Server 2003, Internet Explorer 6.0 for Windows XP Service Pack 2, Windows 98, Windows 98 SE, Windows ME, Internet Explorer 5.5; **Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers**	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-038. These vulnerabilities include: Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability; Similar Method Name Redirection Cross Domain Vulnerability; Install Engine Vulnerability; Drag and Drop Vulnerability; Address Bar Spoofing on Double Byte Character Set Locale Vulnerability; Plug-in Navigation Address Bar Spoofing Vulnerability; Script in Image Tag File Download Vulnerability; SSL Caching Vulnerability. These vulnerabilities could allow remote code execution. **A vulnerability exists in the Microsoft MSN 'heartbeat.ocx' component, used by Internet Explorer on some MSN gaming sites** Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx **Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate()** We are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Security Update CVE Names: CAN-2004-0842 CAN-2004-0727 CAN-2004-0216 CAN-2004-0839 CAN-2004-0844 CAN-2004-0843 CAN-2004-0841 CAN-2004-0845	High	Microsoft Security Bulletin MS04-038, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Notes VU#637760, October 13, 2004, VU#625616, October 15, 2004, VU#431576, VU#630720, & VU#291304, October 18, 2004, VU#673134 & VU#795720, October 19, 2004** **SecurityFocus, October 18, 2004**
Microsoft Office 2000, Excel 2000, Office XP, Excel 2002, Office 2001 for Macintosh, Office v. X for Macintosh	A remote code execution vulnerability exists in Excel. If a user is logged on with administrative privileges, a malicious user who successfully exploited this vulnerability could take complete control of the affected system. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-033.mspx We are not aware of any exploits for this vulnerability.	Microsoft Excel Remote Code Execution CVE Name: CAN-2004-0846	High	Microsoft Security Bulletin MS04-033, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Note VU#274496, October 13, 2004**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0	A remote code execution vulnerability exists in the NetDDE services because of an unchecked buffer. A malicious user who successfully exploited this vulnerability could take complete control of an affected system. However, the NetDDE services are not started by default and would have to be manually started for an attacker to	Microsoft NetDDE Remote Code Execution	High	Microsoft Security Bulletin MS04-031, October 12, 2004

Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows 98, Windows 98 SE, Windows ME; **Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers**	attempt to remotely exploit this vulnerability. This vulnerability could also be used to attempt to perform a local elevation of privileges or remote Denial of Service. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx **Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&execute Transaction=avaya.css.UsageUpdate()** We are not aware of any exploits for this vulnerability.	CVE Name: CAN-2004-0206		US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Note VU#640488, October 13, 2004** **SecurityFocus, October 18, 2004**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange 2000 Server, Exchange Server 2003; **Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers**	A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems, which could let a remote malicious user execute arbitrary code. This vulnerability could potentially affect systems that do not use NNTP. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx **Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&execute Transaction=avaya.css.UsageUpdate()** We are not aware of any exploits for this vulnerability.	Microsoft NNTP Remote Code Execution CVE Name: CAN-2004-0574	High	Microsoft Security Bulletin MS04-036, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **SecurityFocus, October 18, 2004**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003, Datacenter Edition, Windows Server 2003, Enterprise Edition, Windows Server 2003, Standard Edition, Windows Server 2003, Web Edition, Windows 98, Windows 98 SE, Windows ME	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-032. These vulnerabilities include: Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability. These vulnerabilities could permit elevation of privilege, remote code execution, and Denial of Service. **A vulnerability exists in the Windows SetWindowLong and SetWindowLongPtr API function calls. In some cases this can be exploited to gain execution control.** Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Security Update CVE Name: CAN-2004-0207 CAN-2004-0208 CAN-2004-0209 CAN-2004-0211	High	Microsoft Security Bulletin MS04-032, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Notes, VU#910998, VU#218526, VU#806278, October 13, 2004, VU#119262, October 15, 2004**
Microsoft Windows XP Home Edition, XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition	A remote code execution vulnerability exists in Compressed (zipped) Folders because of an unchecked buffer in the way that it handles specially crafted compressed files. A malicious user could exploit the vulnerability by constructing a malicious compressed file that could potentially allow remote code execution if a user visited a malicious web site. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx We are not aware of any exploits for this vulnerability.	Microsoft Compressed (zipped) Folders Remote Code Execution CVE Name: CAN-2004-0575	High	Microsoft Security Bulletin MS04-034, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 **US-CERT Vulnerability Note VU#649374, October 14, 2004**
Multiple Vendors McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV	Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows malicious users to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. Instructions for vendor fixes available at:	Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability	High	iDEFENSE Security Advisory, October 18, 2004

	http://www.idefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true Proofs of Concept exploits have been published.	CVE Names: CAN-2004-0932 CAN-2004-0933 CAN-2004-0934 CAN-2004-0935 CAN-2004-0936 CAN-2004-0937		
NatterChat NatterChat 1.12	An input validation vulnerability exists that could allow a remote malicious user to inject SQL commands. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	NatterChat Input Validation Hole Lets Remote Users Inject SQL Commands	Medium	SecurityTracker Alert ID, 1011692, October 14, 2004
Pinnacle Systems ShowCenter v1.51 build 121	A vulnerability exists which can be exploited by malicious people to conduct Cross-Site Scripting attacks. Invalid input passed to the 'Skin' parameter in 'SettingsBase.php' isn't validated before being returned to the user in a error page. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Pinnacle ShowCenter Skin File Cross-Site Scripting Vulnerability	High	Secunia Advisory ID, SA12613, October 14, 2004
SunGard SCT Campus Pipeline	An input validation vulnerability exists that could allow a remote malicious user to conduct Cross-Site Scripting attacks. The '/cp/render.UserLayoutRootNode.uP' script does not properly validate user-supplied input in the 'utf' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sungard SCT Campus Pipeline Input Validation Error	High	SecurityFocus Bugtraq ID, 11392, October 13, 2004
Symantec Norton Internet Security 2004 Norton Internet Security 2004 Professional Symantec Norton AntiVirus 2004	A vulnerability exists which can be exploited by malicious, local users to disable the auto-protection. The vulnerability is caused due to an error in the auto-protection functionality when dealing with certain Visual Basic scripts. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Symantec Norton AntiVirus Unprivileged Auto-Protection Deactivation	High	Secunia Advisory ID: SA12863, October 18, 2004
viksoe.dk GMail Drive	A vulnerability exists in which a local malicious user could determine the GMail account name and can access the GMail account. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	viksoe.dk GMail Drive Discloses Information and Permits Unauthorized Access	Medium	SecurityTracker Alert ID, 1011758; October 18, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CVE Name: CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004
Apache Software Foundation Conectiva Gentoo HP Immunix Mandrake OpenBSD OpenPKG RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD ?current, 3.4, 3.5	A buffer overflow vulnerability exists in Apache mod_proxy when a 'ContentLength:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200406-16.xml Mandrake: http://www.mandrakesoft.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/ **Fedora Legacy: http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_Proxy Remote Buffer Overflow CVE Name: CAN-2004-0492	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1010462, June 10, 2004 Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:065, June 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004 SGI Security Advisory,

				20040605-01-U, June 21, 2004 **Fedora Legacy Update Advisory, FLSA:1737, October 14, 2004** **US-Cert Vulnerability Note VU#541310, October 19, 2004**
Apache Software Foundation Gentoo Mandrake OpenBSD OpenPKG RedHat SGI Tinysofa Trustix Apache 1.3-2.0.49	A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106 Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org Tinysofa: http://www.tinysofa.org/support/errata/2004/008.html Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200406-05.xml OpenBSD: http://www.openbsd.org/errata.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ Apple: http://www.apple.com/support/security/security_updates.html **Fedora Legacy: http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow CVE Name: CAN-2004-0488	Low/High (High if arbitrary code can be executed)	Security Focus, May 17, 2004 Gentoo Linux Security Advisory, GLSA 200406-05, June 9, 2004 Mandrakelinux Security Update Advisories, MDKSA-2004:054 & 055, June 1. 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.026, May 27, 2004 RedHat Security Advisory, RHSA-2004:342-10, July 6, 2004 SGI Security Advisory, 20040605-01-U, June 21, 2004 Tinysofa Security Advisory, TSSA-2004-008, June 2, 2004 Trustix Security Advisory, TSLSA-2004-0031, June 2, 2004 **Fedora Legacy Update Advisory, FLSA:1888, October 14, 2004**
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Debian: http://security.debian.org/pool/updates/main/c/cyrus-sasl/** We are not aware of any exploits for this vulnerability.	Cyrus SASL Buffer Overflow & Input Validation CVE Name: CAN-2004-0884	High	SecurityTracker Alert ID: 1011568, October 7, 2004 **Debian Security Advisories DSA 563-2, 563-3, & 568-1, October 12 , 14, & 16, 2004**
cPanel, Inc. cPanel 9.4.1-RELEASE-64; 9.9.1-RELEASE-3	Several vulnerabilities exist: a vulnerability exists in the backup feature, which could let a remote authenticated malicious user obtain sensitive information; a vulnerability exists when FrontPage extensions are turned on or off, which could let a remote authenticated malicious user change ownership of critical files; and a vulnerability exists in the '_private' directory when FrontPage extensions are turned on or off, which could let a remote authenticated malicious user change permissions on any file on the target system to 0755. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	cPanel Backup & FrontPage Management Remote Arbitrary File Modifications	Medium/ High (High if root access can be obtained)	SecurityTracker Alert ID, 1011762, October 18, 2004

Federico David Sacerdoti Ansel 1.2, 1.3, 1.4, 2.0	A vulnerability exists due to insecure default permissions when picture albums are created, which could let a remote malicious user obtain unauthorized access. Upgrade available at: http://freshmeat.net/redir/ansel/16337/url_tgz/ansel-2.1.tar.gz There is no exploit code required.	Federico David Sacerdoti Ansel Insecure Default Permissions	Medium	SecurityFocus, October 14, 2004
gnofract4d. sourceforge.net Gnofract 4D prior to 2.2	A vulnerability exists due to an error in the handling of '.fct' parameter files, which could let a remote malicious user execute arbitrary Phyton code. Update available at: http://gnofract4d.sourceforge.net/download.html We are not aware of any exploits for this vulnerability.	Gnofract 4 Remote Arbitrary Code Execution	High	SecurityTracker Alert ID, 1011757, October 17, 2004
libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Proofs of Concept exploits have been published.	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004
Martin Schoenert Unzoo 4.4	A vulnerability exists when a specially crafted archive is created due to insufficient validation, which could let a remote malicious user create or overwrite files. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	unzoo Input Validation	Medium	SecurityTracker Alert ID, 1011673, October 14, 2004
mpg123.de mpg123 0.x	A buffer overflow vulnerability exists in the 'do_layer2()' function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200409-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Debian: http://security.debian.org/pool/updates/non-free/m/mpg123/** An exploit script has been published.	mpg123 'do_layer2() Function' Remote Buffer Overflow CVE Name: CAN-2004-0805	High	Securiteam, September 7, 2004 Gentoo Linux Security Advisory, GLSA 200409-20, September 16, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:100, September 22, 2004 **Debian Security Advisory, DSA 564-1, October 13, 2004**
Mr. S.K. LHA 1.14	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the parsing of archives, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the parsing of command-line arguments, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient validation of shell meta characters in directories, which could let a remote malicious user execute arbitrary shell commands. RedHat: http://rhn.redhat.com/errata/RHSA-2004-323.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-13.xml **Fedora Legacy: http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for these vulnerabilities.	LHA Multiple Code Execution CVE Names: CAN-2004-0694, CAN-2004-0745, CAN-2004-0769, CAN-2004-0771	High	SecurityFocus, September 2, 2004 Fedora Update Notifications FEDORA-2004-294 & 295, September 8, 2004 Gentoo Linux Security Advisory, GLSA 200409-13, September 8, 2004 **Fedora Legacy Update Advisory, FLSA:1833, October 14, 2004**
Multiple Vendors	A vulnerability exists in the 'GRANT' command due to a failure to ensure sufficient privileges, which could let a malicious user obtain unauthorized access.	MySQL Database Unauthorized GRANT	Medium	Trustix Secure Linux Security

MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21.x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.54, 3.23.56, 3.23.58, 3.23.59, 4.0.0-4.0.15, 4.0.18, 4.0.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0, 2.1	Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	Privilege		Advisory, TSLSA-2004-0054, October 15, 2004
Multiple Vendors Conectiva Clearswift Debian F-Secure Fedora Gentoo Mr. S.K. RARLAB RedHat SGI Slackware Stalker WinZip Mr. S.K. LHA 1.14, 1.15, 1.17; RARLAB WinRar 3.20; RedHat lha-1.14i-9.i386. rpm; WinZip 9.0; Stalker CGPMcAfee 3.2	Multiple vulnerabilities exist: two buffer overflow vulnerabilities exist when creating a carefully crafted LHA archive, which could let a remote malicious user execute arbitrary code; and several Directory Traversal vulnerabilities exist, which could let a remote malicious user corrupt/overwrite files in the context of the user who is running the affected LHA utility. RedHat: ftp://updates.redhat.com/9/en/os/i386/lha-1.14i-9.1.i386.rpm Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/non-free/l/lha/ F-Secure: http://www.f-secure.com/security/fsc-2004-1.shtml Fedora: http://www.redhat.com/archives/fedora-announce-list/2004-May/msg00005.html Gentoo: http://security.gentoo.org/glsa/glsa-200405-02.xml SGI: http://www.sgi.com/support/security/ **Fedora Legacy: http://download.fedoralegacy.org/redhat/** Proofs of Concept exploits have been published.	Multiple LHA Buffer Overflow/ Directory Traversal Vulnerabilities CVE Names: CAN-2004-0234, CAN-2004-0235	Medium/ High (High if arbitrary code can be executed)	Conectiva Linux Security Announcement, CLA-2004:840, May 7, 2004 Debian Security Advisory DSA 515-1 , June 5, 2004 F-Secure Security Bulletin, FSC-2004-1, May 26, 2004 Fedora Update Notification, FEDORA-2004-119, May 11, 2004 Gentoo Linux Security Advisory, GLSA 200405-02, May 9, 2004 Red Hat Security Advisory, RHSA-2004:179-01, April 30, 2004 SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004 Slackware Security Advisory, SSA:2004-125-01, May 5, 2004 **Fedora Legacy Update Advisory, FLSA:1833, October 14, 2004**
Multiple Vendors Apple Mac OS X 10.2-10.2.8, 10.3 -10.3.5, OS X Server 10.2-10.2.8, 10.3 -10.3.5; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4-5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.21	A vulnerability exists in 'error_log' when certain methods of remote printing are carried out by an authenticated malicious user, which could disclose user passwords. Update available at: http://www.cups.org/software.php Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04829&platform=osx&method=sa/SecUpd2004-09-30Jag.dmg http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04830&platform=osx&method=sa/SecUpd2004-09-30Pan.dmg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-06.xml **Debian: http://security.debian.org/pool/updates/main/c/cupsys/** There is no exploit code required.	CUPS Error_Log Password Disclosure CVE Name: CAN-2004-0923	Medium	Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004 Fedora Update Notification, FEDORA-2004-331, October 5, 2004 Gentoo Linux Security Advisory, GLSA 200410-06, October 9, 2004 **Debian Security Advisory, DSA 566-1, October 14, 2004**
Multiple Vendors Easy Software	A Denial of Service vulnerability exists in 'scheduler/dirsvc.c' due to insufficient validation of UDP datagrams.	CUPS Browsing Denial of Service	Low	SecurityTracker Alert ID, 1011283, September 15,

Products CUPS 1.1.14-1.1.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	Update available at: http://www.cups.org/software.php Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ ALTLinux: http://altlinux.com/index.php?module=sisyphus&package=cups Gentoo: http://security.gentoo.org/glsa/glsa-200409-25.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Apple: http://www.apple.com/support/security/security_updates.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57646-1&searchclause= **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora Legacy: http://download.fedoralegacy.org/fedora/1/updates/** **SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.15** A Proof of Concept exploit has been published.	CVE Name: CAN-2004-0558		2004 ALTLinux Advisory, September 17, 2004 Gentoo Linux Security Advisory GLSA 200409-25, September 20, 2004 Slackware Security Advisory, SSA:2004-266-01, September 23, 2004 Fedora Update Notification, FEDORA-2004-275, September 28, 2004 Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004 Sun(sm) Alert Notification, 57646, October 7, 2004 **SCO Security Advisory, COSA-2004.15, October 12, 2004** **Conectiva Linux Security Announcement, CLA-2004:872, October 14, 2004** **Fedora Legacy Update Advisory, FLSA:2072, October 16, 2004**
Multiple Vendors OpenBSD 3.4, 3.5; SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8; X.org X11R6 6.7.0, 6.8; XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0	Multiple vulnerabilities exist: a stack overflow exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in -create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ SuSE: ftp://ftp.suse.com/pub/suse/ X.org: http://x.org/X11R6.8.1/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-34.xml IBM: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57652-1&searchclause=** Proofs of Concept exploits have been published.	LibXpm Image Decoding Multiple Remote Buffer Overflow CVE Names: CAN-2004-0687, CAN-2004-0688	High	X.Org Foundation Security Advisory, September 16, 2004 US-CERT Vulnerability Notes, VU#537878 & VU#882750, September 30, 2004 SecurityFocus, October 4, 2004 Debian Security Advisory, DSA 560-1 & 561-1, October 7 & 11, 2004 Gentoo Linux Security Advisory, GLSA 200410-09, October 9, 2004 **Sun(sm) Alert Notification, 57652, October 18, 2004**
MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21 .x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10,	A buffer overflow vulnerability exists in the 'mysql_real_connect' function due to insufficient boundary checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. *Note: Computers using glibc on Linux and BSD platforms may not be vulnerable to this issue.* **Debian: http://security.debian.org/pool/updates/main/m/mysql/** **Trustix: http://http.trustix.org/pub/trustix/updates/**	MySQL Mysql_real_connect Function Remote Buffer Overflow CVE Name: CAN-2004-0836	High/Low (Low if a DoS)	Secunia Advisory, SA12305, August 20, 2004 **Debian Security Advisory, DSA 562-1, October 11, 2004**

3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0.0-4.0.15, 4.0.18, 4.0.20, 4.1 .0-alpha, 4.1 .0-0, 4.1.2 -alpha, 4.1.3 -beta, 4.1.3 -0, 5.0 .0-alpha, 5.0 .0-0	We are not aware of any exploits for this vulnerability.			**Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004**
MySQL AB MySQL 4.0.0-4.0.15, 4.0.18, 4.0.20	A remote Denial of Service vulnerability exists in the 'FULLTEXT' search functionality due to a failure to handle exceptional search input. Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	MySQL Remote Denial of Service	Low	Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004
MySQL AB MySQL 3.x, 4.x	Two vulnerabilities exist: a vulnerability exists due to an error in 'ALTER TABLE ... RENAME' operations because the 'CREATE/INSERT' rights of old tables are checked, which potentially could let a remote malicious user bypass security restrictions; and a remote Denial of Service vulnerability exists when multiple threads issue 'alter' commands against 'merge' tables to modify the 'union.' Updates available at: http://dev.mysql.com/downloads/mysql/ Debian: http://security.debian.org/pool/updates/main/m/mysql **Trustix: http://http.trustix.org/pub/trustix/updates/** We are not aware of any exploits for these vulnerabilities.	MySQL Security Restriction Bypass & Remote Denial of Service CVE Names: CAN-2004-0835, CAN-2004-0837	Low/ Medium (Low if a DoS; and Medium if security restrictions can be bypassed)	Secunia Advisory, SA12783, October 11, 2004 **Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004**
phpMyAdmin phpMyAdmin 2.0-2.0.5, 2.1-2.1.2, 2.2, 2.2 pre1&2, 2.2 rc1-rc3, 2.2.2-2.2.6, 2.3.1, 2.3.2, 2.4 .0, 2.5 .0-2.5.2, 2.5.4, 2.5.5 pl1. 2.5.5 -rc1&rc2, 2.5.5, 2.5.6 -rc1, 2.5.7 pl1, 2.5.7, 2.6.0pl1	A vulnerability exists in the MIME-based transformation system with 'external' transformations, which could let a remote malicious user execute arbitrary code. *Note: Successful exploitation requires that PHP's safe mode is disabled.* Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=23067&package_id=16462&release_id=274709 Gentoo: http://security.gentoo.org/glsa/glsa-200410-14.xml There is no exploit code required.	phpMyAdmin Remote Command Execution	High	Secunia Advisory, SA12813, October 13, 2004
PNG Development Group Conectiva Debian Fedora Gentoo Mandrakesoft RedHat SuSE Sun Solaris HP-UX GraphicsMagick ImageMagick Slackware libpng 1.2.5 and 1.0.15	Multiple vulnerabilities exist in the libpng library which could allow a remote malicious user to crash or execute arbitrary code on an affected system. These vulnerabilities include: • libpng fails to properly check length of transparency chunk (tRNS) data, • libpng png_handle_iCCP() NULL pointer dereference, • libpng integer overflow in image height processing, • libpng png_handle_sPLT() integer overflow, • libpng png_handle_sBIT() performs insufficient bounds checking, • libpng contains integer overflows in progressive display image reading. If using original, update to libpng version 1.2.6rc1 (release candidate 1) available at: http://www.libpng.org/pub/png/libpng.html Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000856 Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00139.html Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079 RedHat http://rhn.redhat.com/ SuSE: http://www.suse.de/de/security/2004_23_libpng.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Sun Solaris: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57617 HP-UX: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01065 GraphicsMagick: http://www.graphicsmagick.org/www/download.html ImageMagick: http://www.imagemagick.org/www/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243 Yahoo: http://messenger.yahoo.com/	Multiple Vulnerabilities in libpng CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599	High	US-CERT Technical Cyber Security Alert TA04-217A, August 4, 2004 US-CERT Vulnerability Notes VU#160448, VU#388984, VU#817368, VU#236656, VU#477512, VU#286464, August 4, 2004 SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004 **SCO Security Advisory, SCOSA-2004.16, October 12, 2004**

	SuSE: ftp://ftp.suse.com/pub/suse **SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.16** A Proof of Concept exploit has been published.			
ProFTPd.net ProFTPd 1.2.8, 1.2.10; possibly other versions	A vulnerability exists due to a time delay difference in the login process for existing and non-existing usernames, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	ProFTPd Login Timing Account Disclosure	Medium	LSS Security Team Advisory, October 14, 2004
Samba.org Samba version 3.0 - 3.0.6	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in the 'process_logon_packet()' function due to insufficient validation of 'SAM_UAS_CHANGE' request packets; and a remote Denial of Service vulnerability exists when a malicious user submits a malformed packet to a target 'smbd' server. Updates available at: http://samba.org/samba/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-467.html **Conectiva: ftp://atualizacoes.conectiva.com.br/** We are not aware of any exploits for these vulnerabilities.	Samba Remote Denials of Service CVE Names: CAN-2004-0807, CAN-2004-0808	Low	Securiteam, September 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-16, September 13, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:092, September 13, 2004 Trustix Secure Linux Bugfix Advisory, TSL-2004-0046, September 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.040, September 15, 2004 SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004 RedHat Security Advisory, RHSA-2004:467-08, September 23, 2004 **Conectiva Linux Security Announcement, CLA-2004:873, October 14, 2004**
sox.sourceforge.net Fedora Mandrakesoft Gentoo Conectiva RedHat SoX 12.17.4, 12.17.3, and 12.17.2	Multiple vulnerabilities exist that could allow a remote malicious user to execute arbitrary code This is due to boundary errors within the "st_wavstartread()" function when processing ".WAV" file headers and can be exploited to cause stack-based buffer overflows. Successful exploitation requires that a user is tricked into playing a malicious ".WAV" file with a large value in a length field. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:076 Gentoo: http://security.gentoo.org/glsa/glsa-200407-23.xml Conectiva: ftp://atualizacoes.conectiva.com.br RedHat: http://rhn.redhat.com/errata/RHSA-2004-409.html Slackware: ftp://ftp.slackware.com/pub/slackware/ SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ **Debian: http://security.debian.org/pool/updates/main/s/sox/** An exploit script has been published.	SoX ".WAV" File Processing Buffer Overflow Vulnerabilities CVE Name: CAN-2004-0557	High	Secunia, SA12175, 12176, 12180, July 29, 2004 SecurityTracker Alerts 1010800 and 1010801, July 28/29, 2004 Mandrakesoft Security Advisory MDKSA-2004:076, July 28, 2004 PacketStorm, August 5, 2004 Slackware Security Advisory, SSA:2004-223-03, august 10, 2004 SGI Security Advisory, 20040802-01-U, August 14, 2004

				Debian Security Advisory, DSA 565-1, October 13, 2004
Squid-cache.org Squid 2.5-STABLE6, 3.0-PRE3-20040702; when compiled with SNMP support	A remote Denial of Service vulnerability exists in the 'asn_parse_header()' function in 'snmplib/asn1.c' due to an input validation error when handling certain negative length fields. Updates available at: http://www.squid-cache.org/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **Gentoo: http://security.gentoo.org/glsa/glsa-200410-15.xml** **Trustix: http://http.trustix.org/pub/trustix/updates/** We are not aware of any exploits for this vulnerability.	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	iDEFENSE Security Advisory, October 11, 2004 **Fedora Update Notification, FEDORA-2004-338, October 13, 2004** **Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004** **Gentoo Linux Security Advisory, GLSA 200410-15, October 18, 2004**
Sun Microsystems, Inc. Solaris 8	A vulnerability exists in the gzip(1) command, which could let a malicious user access the files of other users that were processed using gzip. Workaround and update available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57600-1 We are not aware of any exploits for this vulnerability.	Sun Solaris Gzip File Access	Medium	Sun(sm) Alert Notification, 57600, October 1, 2004 **US-CERT Vulnerability Note VU#635998, October 18, 2004**
Todd Miller Sudo 1.6.8	A vulnerability exists due to insufficient validation of symbolic links when sudoedit ("sudo -u" option) copies temporary files, which could let a malicious user access the contents of arbitrary files with superuser privileges. Upgrade available at: ftp://ftp.sudo.ws/pub/sudo/sudo-1.6.8p1.tar.gz There is no exploit code required; however, a Proof of Concept exploit script has been published.	Sudo Information Disclosure	High	Secunia Advisory, SA12596, September 20, 2004 **US-CERT Vulnerability Note VU#424358, October 19, 2004**
WeHelpBUS WeHelpBUS 0.1	A vulnerability exists in 'wehelpbus/sk.cgi.in,' 'wehelpbus/skdoc.cgi.in,' 'wehelpbus/wehelpbus.pl.in,' 'wehelpbus/info.cgi.in,' 'wehelpbus/man.cgi.in,' 'wehelpbus/rpm.cgi.in,' and 'wehelpbus/code.cgi.in,' which could let a remote malicious user execute arbitrary commands. Upgrade available at: http://prdownloads.sourceforge.net/wehelpbus/wehelpbus-0.2.tar.gz?download There is no exploit code required.	WeHelpBUS Input Validation	High	SecurityTracker Alert ID, 1011743, October 16, 2004
Yukihiro Matsumoto Ruby 1.6, 1.8	A vulnerability exists in the CGI session management component due to the way temporary files are processed, which could let a malicious user obtain elevated privileges. Upgrades available at: http://security.debian.org/pool/updates/main/r/ruby/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-08.xml RedHat: http://rhn.redhat.com/errata/RHSA-2004-441.html **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** We are not aware of any exploits for this vulnerability.	Ruby CGI Session Management Unsafe Temporary File CVE Name: CAN-2004-0755	Medium	Debian Security Advisory, DSA 537-1, August 16, 2004 Gentoo Linux Security Advisory, GLSA 200409-08, September 3, 2004 RedHat Security Advisory, RHSA-2004:441-18, September 30, 2004 **Fedora Update Notification, FEDORA-2004-264, October 15, 2004**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
3Com OfficeConnect ADSL Wireless 11g Firewall Router 1.13 firmware, 1.23 firmware, 1.24	Several vulnerabilities exist: an unspecified security issue exists which may cause duplicate login IPs to be displayed; an unspecified error exists in the DHCP service; and a remote Denial of Service vulnerability exists due to an unspecified boundary error. Upgrades available at:	3Com OfficeConnect ADSL Wireless 11g Firewall Router Multiple Vulnerabilities	Low	Secunia Advisory, SA12796, October 15, 2004

firmware	http://webprd1.3com.com/swd/jsp/user/index.jsp?id=OCFR4 Currently, we are not aware of any exploits for this vulnerability.			
3Com 3CRADSL72 Wireless Router	A vulnerability exists when a remote malicious user connects to a certain web page, which could lead to the disclosure of sensitive information and administrative access. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit has been published.	3Com 3CRADSL72 ADSL Wireless Router Information Disclosure & Authentication Bypass	Medium/ High (High if administrative access can be obtained)	Bugtraq, October 15, 2004
Alivesites Forum 2.0	Multiple input validation vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input before used in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required	AliveSites Forum Multiple Unspecified Remote Input Validation	High	Secunia Advisory, SA12844, October 15, 2004
ASN.1 ASN.1 Compiler 0.9.4	Several vulnerabilities exist: a vulnerability exists in 'OCTET_STRING.c'. when processing ANY type tags; and a vulnerability exists due to the way CHOICE types are handled when extensions have indefinite length structures. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=103893&package_id=111693&release_id=274592 We are not aware of any exploits for these vulnerabilities.	ASN1 Multiple Vulnerabilities	Not Specified	Secunia Advisory, SA12794, October 12, 2004
clientexec.com ClientExec 2.2.1	A vulnerability exists because 'phpinfo.php' is installed in the main ClientExec directory, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ClientExec Default Installation Information Disclosure	Medium	Secunia Advisory, SA12862, October 18, 2004
cphp.sourceforge.net CoolPHP Web Portal 1.0 - stable	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'index.php' due to insufficient sanitization of the 'query' and 'nick' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'index.php' due to insufficient verification of the 'op' parameter, which could let a remote malicious user include arbitrary files from local resources; and a vulnerability exists in 'index.php' when an invalid 'op' value is submitted, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	CoolPHP Multiple Remote Input Validation	Medium/ High (High if arbitrary code can be executed)	CHT Security Research Center-2004, October 16, 2004
DevoyBB DevoyBB Web Forum 1.0	Multiple input validation vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input before used in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required	DevoyBB Forum Multiple Unspecified Remote Input Validation	High	SecurityFocus, October 15, 2004
Express-Web Content Management System	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required	Express-Web Content Management System Cross-Site Scripting	High	Secunia Advisory, SA12839, October 15, 2004
FuseTalk Inc. FuseTalk 4.0	A Cross-Site Scripting vulnerability exists due to insufficient validation of user-supplied input in the IMG tag, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	FuseTalk Cross-Site Scripting	High	SecurityTracker Alert ID, 1011664, October 13, 2004
GoSmart Inc. GoSmart Message Board	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of the 'QuestionNumber' and 'Category' parameters in 'Forum.asp,' and the 'Username' and 'Password' parameters in 'Login_Exec.asp,' which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists due to insufficient sanitization of the 'Category' parameter in 'Forum.asp' and the 'MainMessageID' parameter in 'ReplyToQuestion.asp,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	GoSmart Message Board Multiple Input Validation	High	MAxpatrol Security Advisory, October 11, 2004
IBM DB2 Universal Database	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'DB2LPORT' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code; a buffer overflow**	IBM DB2 Multiple Buffer Overflows	High	NGSSoftware Insight Security Research

for AIX 8.0, 8.1, DB2 Universal Database for HP-UX 8.0, 8.1, DB2 Universal Database for Linux 8.0, 8.1, DB2 Universal Database for Solaris 8.0, 8.1, DB2 Universal Database for Windows 8.0, 8.1	**vulnerability exists due to insufficient validation uf user-supplied string length before copying them into finity process buffers, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'DB2FMP' command due to insufficient bounds checking, which could let a malicious user execute arbitrary code; multiple buffer overflow vulnerabilities exist in the DB2 Application Programming Interface (API), which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists due to insufficient bounds checking of library names, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'sqlvGenDtsFormat()' function when DTS to string conversion is carried out; a buffer overflow vulnerability exists in 'JDBC' requests due to insufficient bounds checks, which could let a remote malicious user execute arbitrary code; a vulnerability exists (only on Windows operating systems) because local malicious users can inappropriately connect to IPC resources, which could lead to the disclosure of sensitive information; a Denial of Service vulnerability exists when DB2 is installed on Microsoft Windows operating systems due to a failure to properly ensure that only authorized users can signal the DB2 UDB instance to shutdown; a buffer overflow vulnerability exists due to insufficient bounds checking of data that is handled through XML Extender UDF's, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists in the universal Database Security Service due to a failure to handle malformed network messages (Windows operating systems only).** Patches available at: http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html We are not aware of any exploits for these vulnerabilities.			Advisory, October 5, 2004 **SecurityFocus, October 13, 2004**
Macromedia JRun 3.0, 3.1, 4.0,	Multiple vulnerabilities exist: a vulnerability exists due to an implementation error in the generation and handling of JSESSIONIDs, which could let a remote malicious user hijack an authenticated user's session; a Cross-Site Scripting vulnerability exists in the JRUN Management Console, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to an URL parsing error, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists in the verbose logging module. Patches available at: http://www.macromedia.com/support/jrun/updaters.html We are not aware of any exploits for these vulnerabilities.	Macromedia JRun Multiple Remote Vulnerabilities	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Macromedia Security Bulletin, MPSB04-08, September 23, 2004 **US-CERT Vulnerability Notes VU#977440, VU#584958, & VU#668206, October 12, 2004, VU#990200, October 14, 2004**
Motorola WR850G 4.0 3 firmware	A vulnerability exists due to an error in the session handling, which could let a remote malicious user execute arbitrary commands with administrative privileges; and a vulnerability exists which could let a remote malicious user access the 'frame_debug.asp' page to obtain shell access on the system. **Upgrade available at:** **http://broadband.motorola.com/consumers/products/WR850g/downloads/Motorola_WR850G_5.13.exe** There is no exploit code required.	Motorola Wireless Router WR850G Authentication Circumvention	High	SecurityTracker Alert ID, 1011413, September 26, 2004 **SecurityFocus, October 13, 2004**
Multiple Vendors	A vulnerability exists due to the way some networking devices store cookies on a user's system when the 'Secure' attribute is not set, which could let a remote malicious user obtain sensitive information. Patches and update information available at: http://www.kb.cert.org/vuls/id/546483 We are not aware of an exploit for this vulnerability.	Multiple Networking Devices 'Secure' Cookie Attribute Failure CVE Name: CAN-2004-0462	Medium	US-CERT Vulnerability Note VU#546483, October 18, 2004
ocportal.com Ocportal Web Content Management System 1.0-1.0.3	A vulnerability exists in 'index.php' due to insufficient verification of the 'reg_path' parameter, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ocportal.com/dload.php?id=32 There is no exploit code required.	ocPortal 'index.php' Remote Code Execution	High	hackgen-2004-#002, October 12, 2004
phpWebSite Development Team phpWebsite 0.7.3, e 0.8.2, 0.8.3, 0.9.3 -4, 0.9.3	Multiple input validation vulnerabilities exist: a vulnerability exists in 'index.php' due to insufficient sanitization of the 'pid' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the calendar module due to insufficient sanitization of the 'cal_template' field, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient sanitization of input passed to the subject and message fields, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.phpwebsite.appstate.edu/downloads/security/phpwebsite-core-security-patch.tar.gz There is no exploit code required; however, a Proof of Concept exploit script has	PHPWebSite Multiple Input Validation CVE Names: CAN-2003-0735, CAN-2003-0736	High	GulfTech Security Research Security Advisory, August 31, 2004 **US-CERT Vulnerability Note VU#925166 & VU#664422, October 19,**

	been published.			**2004**
Research In Motion Limited BlackBerry Wireless Handheld 3.7.1.41; Model 7230	A remote Denial of Service vulnerability exists in the 'Location' field due to a failure to handle meeting request messages with a string larger than 128KB. The vulnerability has been fixed in BlackBerry handheld software version 3.8. We are not aware of any exploits for this vulnerability.	Blackberry Operating System Remote Denial of Service	Low	Secunia Advisory, SA12814, October 15, 2004
The BNC Project BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2, 2.8.8	A buffer overflow vulnerability exists due to a flaw when processing the backspace character, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www.gotbnc.com/files/bnc2.8.9.tar.gz **Gentoo: http://security.gentoo.org/glsa/glsa-200410-13.xml** We are not aware of any exploits for this vulnerability.	BNC Buffer Overflow	High	SecurityTracker Alert ID, 1011583, October 9, 2004 **Gentoo Linux Security Advisory, GLSA 200410-13, October 15, 2004**
Thomas Ehrhardt Powies PSCRIPT Forum 1.26 & prior	Several input validation vulnerabilities exist due to insufficient sanitization of user-supplied input to the 'logincheck.php,' 'changepass.php,' and 'edituser.php' scripts, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Powie's PSCRIPT Forum Input Validation	High	Secunia Advisory, SA12868, October 19, 2004
Veritas Veritas Cluster Server 4.0 & prior	A vulnerability exists due to an unspecified error, which could let a malicious user execute arbitrary code with root privileges. Update available at: http://seer.support.veritas.com/docs/ We are not aware of any exploits for this vulnerability.	VERITAS Cluster Server Remote Code Execution	High	Secunia Advisory, SA12833, October 15, 2004
wikipedia. sourceforge.net MediaWiki prior to 1.3.6	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of input passed in UnicodeConverter extension and 'raw' page view, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient sanitization of input passed to 'Specialblcoklist,' 'SpecialEmailuser,' 'SpecialMaintenance,' and 'ImagePage,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'SpecialMaintenance' due to insufficient verification, which could let a remote malicious user manipulate SQL queries. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=34373 We are not aware of any exploits for these vulnerabilities.	MediaWiki Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA12825, October 14, 2004
WordPress WordPress 1.2	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient verification of user-supplied input passed to certain parameters in various scripts, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://wordpress.org/latest.tar.gz **Gentoo: http://security.gentoo.org/glsa/glsa-200410-12.xml** There is no exploit code required; however, Proofs of Concept exploits have been published.	Wordpress Multiple Cross-Site Scripting	High	Bugtraq, September 27, 2004 Secunia Advisory, SA12773, October 11, 2004 **Gentoo Linux Security Advisory, GLSA 200410-12, October 14, 2004**
WowBB WowBB Web Forum	Multiple input validation vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of unspecified input before used in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required	WowBB Forum Multiple Unspecified Remote Input Validation	High	SecurityFocus, October 15, 2004
yahoopops.sourceforge.net YPOPs! 0.x	Several buffer overflow vulnerabilities exist in the POP3 and SMTP services, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **Proofs of Concept exploit scripts have been published.**	YPOPs! Buffer Overflows	High	Hat-Squad Advisory, September 27, 2004 **SecurityFocus, October 18, 2004**
yapig.sourceforge.net YaPiG prior to 0.92.2b	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://sourceforge.net/project/shownotes.php?release_id=275720	YaPiG Input Validation	High	Secunia Advisory, SA12858, October 18, 2004

	A Proof of Concept exploit has been published.			

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
October 18, 2004	yahoopops.c 101_ypops.cpp dc_ypop.c	No	Exploits for the YPOPs! Buffer Overflows vulnerabilities.
October 15, 2004	proftpd.c	No	Script that exploits the ProFTPd Login Timing Differences Disclose Valid User Account Names vulnerability.
October 13, 2004	sessmgr.c	No	Script that exploits the Microsoft Windows XP Weak Default Configuration vulnerability.
October 13, 2004	shixxbof.zip	No	Exploit for the ShixxNOTE 6.net Remote Buffer Overflow vulnerability.

[back to top]

Trends

- Multiple vendors' networking devices fail to set the "Secure" cookie attribute and could disclose sensitive information about a user's HTTP session. Many networking devices provide a built-in web server, which may support the HTTPS protocol. When a user logs into the device with a username/password via HTTP, a cookie may be stored for that session by the web application. When storing this cookie, the "Secure" attribute should be set so that the user-agent only sends this cookie over secure connections (i.e. HTTPS). For more information, see US-CERT Vulnerability Note VU#546483 located at: http://www.kb.cert.org/vuls/id/546483.
- CipherTrust, an e-mail security company, in a survey this month of more than 4 million pieces of e-mail found that most phishing attempts come from about 1000 compromised "zombie" computers owned by broadband customers, and the phishing attacks are likely generated by less than five phishing operations. For more information, see "Has Your PC Gone Phishing?" located at: http://www.pcworld.com/news/article/0,aid,118171,00.asp.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Netsky-B	Win32 Worm	Stable	February 2004
7	Netsky-Q	Win32 Worm	Stable	March 2004
8	MyDoom-O	Win32 Worm	Stable	July 2004
9	Bagle-Z	Win32 Worm	Stable	April 2004
10	MyDoom.M	Win32 Worm	Stable	July 2004

Table Updated October 19, 2004

Viruses or Trojans Considered to be a High Level of Threat

- Netsky.AG - A new variant of the Netsky virus has been discovered and rated as a medium risk by some anti-virus vendors. Like other Netsky viruses, W32/Netskyag@MM uses an e-mail to gain entry and install itself into several files via the Windows directory. Once installed, it harvests e-mail addresses from the infected machine and sends out copies of itself in messages. The virus differs from earlier versions in that it uses different compression technologies when sending itself out. This makes it more difficult to detect. (CNET News.com, October 14, 2004)

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Bifrose	BackDoor-CKA Backdoor.Win32.Bifrose.d	Trojan

Backdoor.Hacarmy.E	BackDoor-AZV.gen	Trojan
Backdoor.Yiha		Trojan
Bacros.A	W32/Bacros.A W97M/Bacros.A Win32.Bacros.a	Win32 Worm
Darby.gen	W32/Darby.gen.worm	Win32 Worm
Downloader-QV		Trojan
HTML.Phishbank.BY	HTML/Phishbank.711.Trojan HTML_CITIFRAUD.C Phish-BankFraud.eml TrojanSpy.HTML.Citifraud.ai	E-mail Phishing Scam
Mydoom.AD	W32/Mydoom.AD.worm	Win32 Worm
Mydoom.AF	I-Worm.Mydoom.AA MyDoom.AE W32.Mydoom.AF@mm W32/Mydoom.ae@MM Win32.Mydoom.AD Win32/Mydoom.AD.DLL.Worm Win32/Scran.Worm	Win32 Worm
Netsky.AG	W32/Netsky.AG.worm	Win32 Worm
Trojan.Webus.C		Trojan
W32.Bacros		Win32 Worm
W32.Darby.B		Win32 Worm
W32.Narcs		Win32 Worm
W32.Nits.A	Worm.Win32.Randin.c	Win32 Worm
W32.Spybot.FBG	WORM_SDBOT.WC	Win32 Worm
W32.Syphilo	W32.Sophily	Win32 Worm
W32/Bagz.d@MM		Win32 Worm
W32/Forbot-AZ	WORM_WOOTBOT.GEN	Win32 Worm
W32/Forbot-BI	WORM_WOOTBOT.AQ	Win32 Worm
W32/Forbot-BN		Win32 Worm
W32/Forbot-BP		Win32 Worm
W32/Netsky-AD		Win32 Worm
W32/Rbot-NA	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NC	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.j	Win32 Worm
W32/Rbot-ND	Backdoor.Win32.Rbot.gen W32/Spybot.worm.gen.e WORM_SDBOT.WK	Win32 Worm
W32/Sdbot-QF	Backdoor.Win32.Wootbot.gen WORM_WOOTBOT.BB W32/Sdbot.worm.gen.h	Win32 Worm
W32/Sdbot-QG	Backdoor.Win32.SdBot.gen W32/Sdbot.worm.gen.h	Win32 Worm
W32/Sdbot-QH	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Sdbot-QJ		Win32 Worm
W32/Sluter-E		Win32 Worm
W32/Traxg-B	WORM_VB.F	Win32 Worm
W32/Traxg-B		Win32 Worm
W32/Wort-B	Exploit.Win32.RPCLsa.10 Exploit-MS04-011.gen	Win32 Worm
Win32.Agni.864	W32/Anies W95.Doggie.gen Win32.Butitil.864 Win32/Agniezhka	Win32 Worm
Win32.Blackmal.E	I-Worm.Nyxem.d W32.Blackmal.C@mm W32/MyWife.c@MM W32/Nyxem.D@mm Win32/Blackmal.E.Worm	Win32 Worm
Win32.Revcuss.D	BackDoor-CHN.gen Backdoor/Revcuss.D.Server	Win32 Worm
WORM_NETSKY.AF	I-Worm.NetSky.b Netsky.AE NetSky.AF W32.Netsky.AD@mm W32/Netsky-AD W32/Netsky.ag@MM Win32.Netsky.AE Win32.Netsky.AE!ZIP Win32/Netsky.AE.Worm	Win32 Worm
WORM_WOOTBOT.BJ	W32/Sdbot.AYN.worm W32/Spybot.BAQ	Win32 Worm

[back to top]

Last updated October 20, 2004